
Cybersecurity: Awareness, Preparedness and Strategy

Doug Johnson
American Bankers Association

Agenda

- What Are The Threats
- ABA Cyber Resources
- The Path Forward – 2014/15

Preferred Banking Method 2013
U.S. adults 18+



What are the Threats

- Denial-of-Service Attacks
- Account Takeovers
- Website (SQL) Injections
- Point-of-Sale Breaches





UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI Cyber Division

Private Industry Notification

30 August 2013

PIN #: 130830 - 001

(U) Hacktivist Group Targeting Financial Institution Web Sites with Distributed Denial of Service Attacks

(U) General Observations:

(U) The FBI is aware of a possible cyber-related threat to financial institutions beginning September 1, 2013. On August 27, 2013, the hacktivist group "Tunisian Hackers II" updated their Facebook page (<http://www.facebook.com/tunisianhackers2>) with information on "Phase I" of OpUSA, an effort to target several commercial and government sites with distributed denial of service (DDoS) attacks. "Phase II", a day devoted to wide-spread web defacements, will then commence on September 11, 2013.

(U) Planned Phase I Targets

(U) Phase 1 of OpUSA will consist of 10 days of DDoS attacks against a specific bank each day between September 1-10. According to a post made on pastebin.fr/28528, the planned targets are as follows:

09/01/2013
<https://www.com>
IP: 171.222.254.100

09/02/2013
<http://www.com>
IP: 161.149.128.100

09/03/2013
<http://www.unitedbank.com>
IP: 74.200.56.18

09/06/2013
<http://www.rbcbank.com>
IP: 142.245.97.214

09/07/2013
<http://www.securitybankusa.com>
IP: 54.236.189.64

09/08/2013
<https://www.royalbank-usa.com/>
IP: 74.200.57.147





- ▶ By Job Function
- ▶ By Bank Type
- ▶ E-mail Bulletins

Home > Tools & Resources > By Job Function > Fraud / Security > Distributed Denial of Service Attacks (DDoS)



Distributed Denial of Service Attacks (DDoS)

August 2013

FBI Warns of OpUSA Cyber Attacks

On August 30, the FBI warned financial institutions to take precautionary measures in anticipation of distributed denial of service attacks, or DDoS, that criminal hackers have planned for this month. Most of the targets of the attacks, which are expected to comprise Phase I of an effort known as "OpUSA," are U.S. government agencies and financial institutions.

A Tunisian hacktivist website shows that Phase I, which began Sept. 1, will consist of 10 days of DDoS attacks against a specific bank each day, the FBI said in an alert shared with ABA. Phase II will commence on Sept. 11 and feature a more widespread attack. The FBI said precautionary measures include implementing a data back-up and recovery plan; readying a DDoS mitigation strategy; regularly mirroring and maintaining an image of critical system files; and scrutinizing links contained in email attachments.

Read the FBI alert. <http://www.aba.com/Tools/Ebulletins/Mem/Documents/OpUSAPIN20130830.pdf> (Members Only)

On August 5, the criminal hackers associated with OpUSA created a new Pastebin post identifying new targets, mostly U.S. government agencies and financial institutions, for their next attack slated for September 11. OpUSA is the group behind the distributed denial of service (DDoS) attacks launched against financial institutions in May 2013 which were deemed to be poorly coordinated and resulting in little to no impact to the sector. Per an alert from the Financial Services Information Sharing and Analysis Center (FS-ISAC), the latest OpUSA campaign most likely will rely on commercial tools to exploit known vulnerabilities, rather than developing custom tools or exploits. This suggests some of the participants possess rudimentary hacking skills capable of causing only temporary disruptions of targeted websites.

See the [FS-ISAC announcement](#). ☺

If you experience activity related to OpUsa, please contact the [FS-ISAC SOC](#).



Denial of Service - Goals

- **Disruption**
 - Cause damage to business income / reputation
- **Demonstration**
 - Assert superiority
 - Publicize a cause
- **Diversion**
 - Divert attention from an illicit act
 - *Applies almost exclusively to financial transactions*
- **Destruction?**

Evolution from Disruptive to Destructive Attacks

Advanced DDOS – 2012, 2013

- 40+ FIs targeted
- Resulted in dynamic, effective information sharing
- Wake up call for financial services industry

Shamoon – 2012

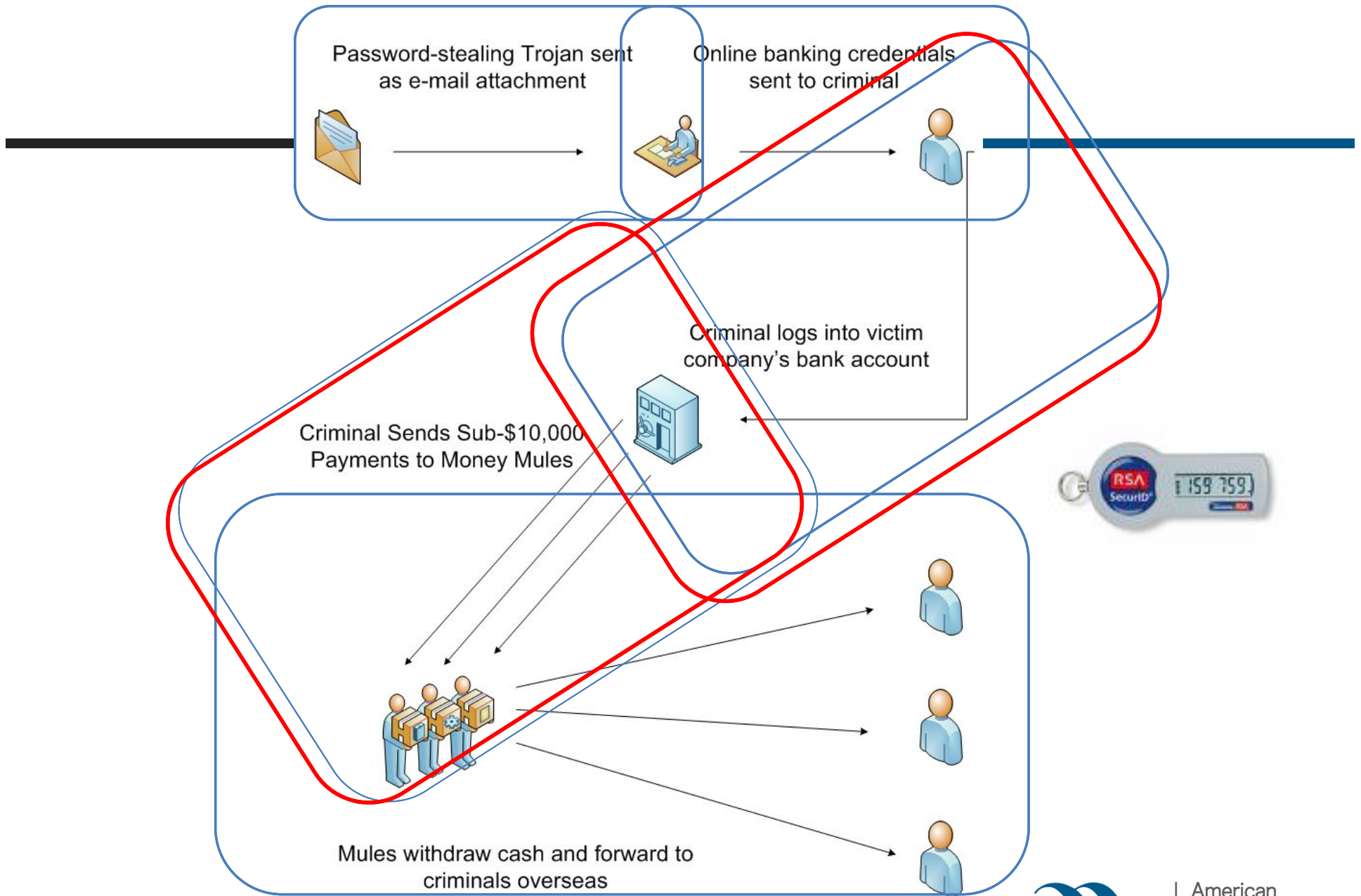
- Malware executable spread using network shared drives
- Corrupts files and wipes device boot blocks at specified date
- A group named "Cutting Sword of Justice" claimed responsibility
- Attack on 30,000 Saudi Aramco workstations

South Korean Attacks – 2013

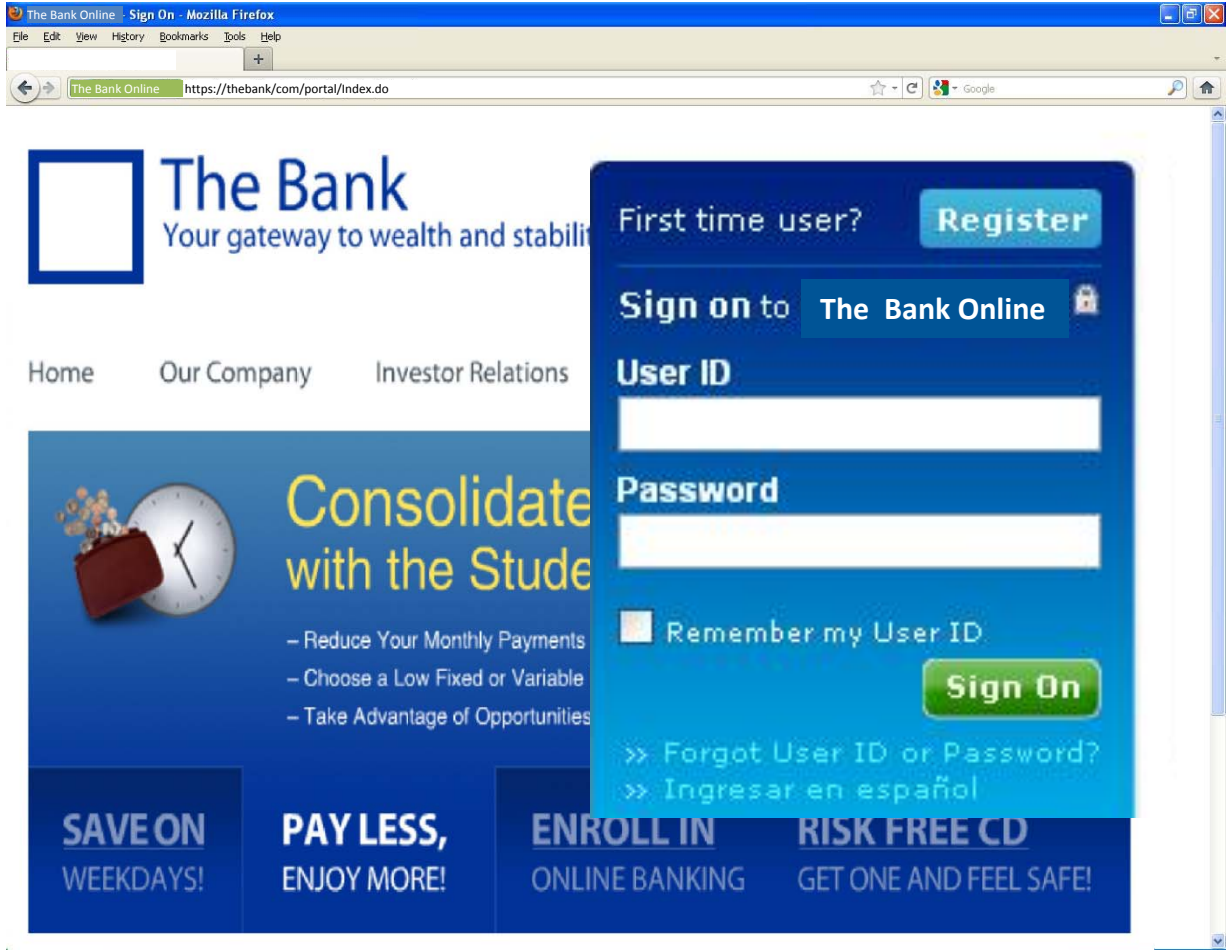
- 2 banks, media company and insurance company targeted
- Patch systems targeted
- Wipers hit Windows, Linux and UNIX OS and removed system files. Over 3,000 machines made unbootable

Would You Click on This Link?

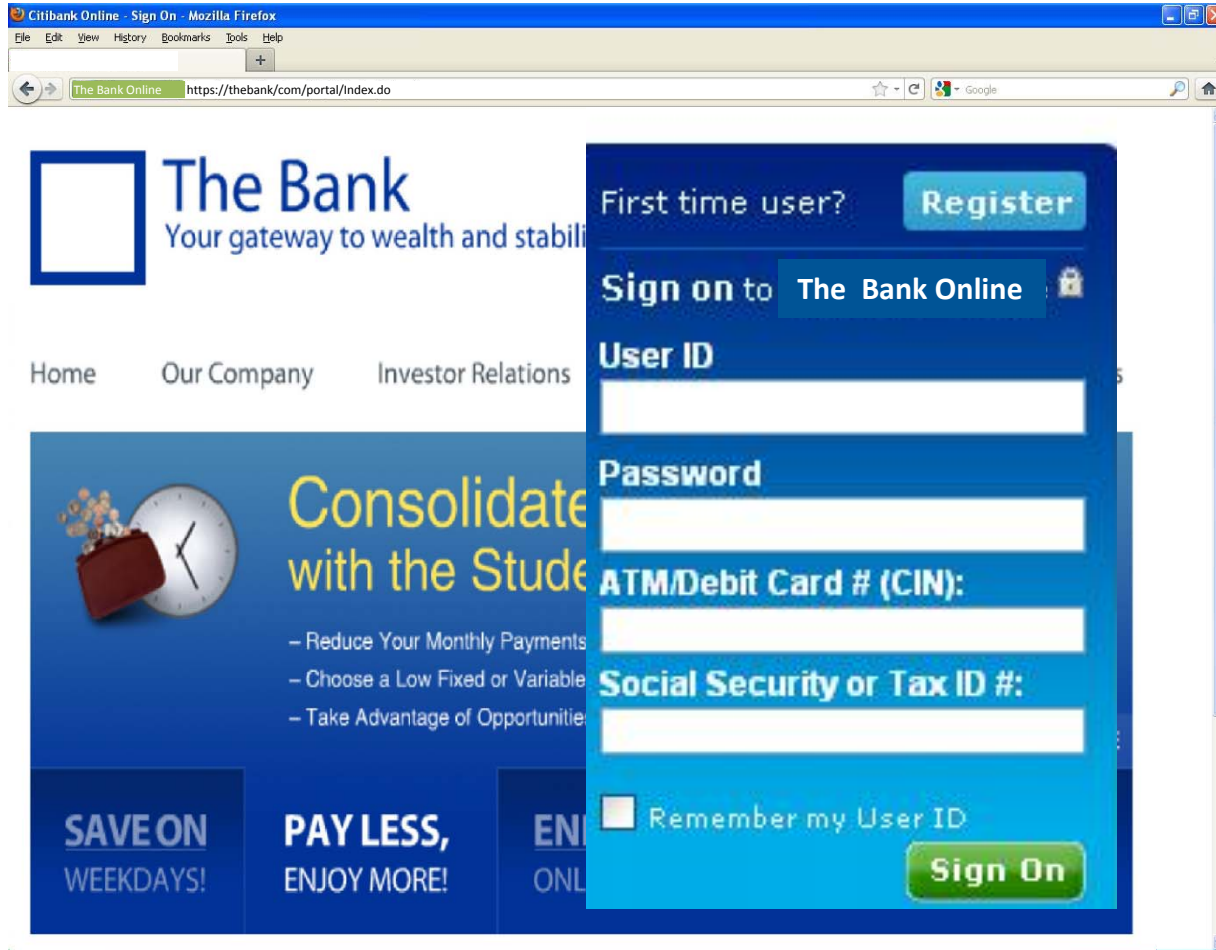




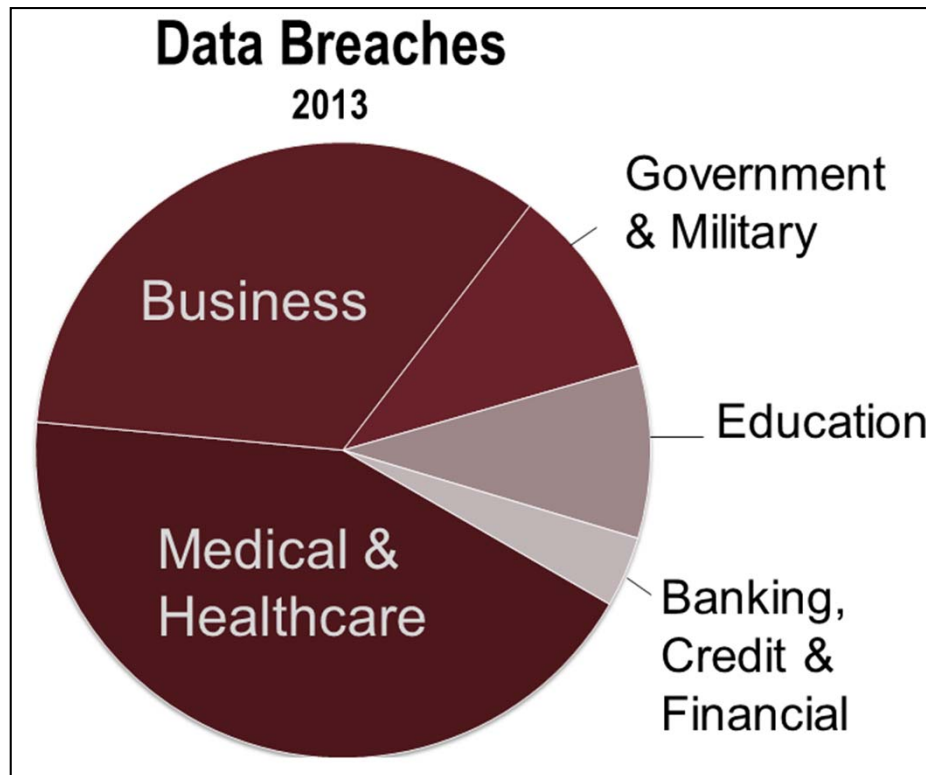
Actual Bank Site



Infected Bank Site



Where do Breaches Occur?



Source: Identity Theft Resource Center

- There were over 600 reported data breaches during 2013
- The two sectors reporting the highest number of breaches were the healthcare sector at 43 percent of reported breaches and the business sector, including merchants, which accounted for nearly 34 percent of reported breaches.
- The business sector, because of the Target breach, accounted for almost 82 percent of 2013's breached records.
- The Banking, Credit and Financial sector accounted for 4 percent of all breaches and less than 2 percent of all breached records.
- ***Overall, for 2009, 62 percent of reported debit card fraud losses were borne by banks, while 38 percent were borne by merchants.***

ABA Resources

Network Security and Data Protection



Corporation for American Banking, L.L.C.

Cybersecurity Resources off Homepage

The screenshot displays the American Bankers Association (ABA) website homepage. At the top left is the ABA logo and the text "American Bankers Association". To the right are links for "Sign out", "Contact Us", "Press Room", and "Consumers", along with a search bar. A dark blue navigation bar contains the following menu items: "About ABA", "Training & Events", "Policy Issues", "Advocacy", "Compliance", "Tools & Resources", "Products", and "Bank Community Engagement".

The main content area features a large banner image of a family in a field. Overlaid on the right side of the banner is a yellow box with the text: "WE CAN'T DREAM BIG ENOUGH" and "ABA National Agricultural Bankers Conference November 10-13, 2013".

Below the banner is a row of social media icons. To the right of the banner is a user profile section for "Doug Johnson" with options to "Manage E-Bulletins", "Update Your Info", and "Log Out". Below this is a "Your Committees" section listing "Bank Security Committee", "Community Bankers Council", and "Information Security".

Further down is a "Get Started" section with a checked box and a list of links: "Login", "Compliance calendar", "Training", "Trending issues", "Resources by Job Function", "Register for a conference", "Online courses", "Certifications", and "Join ABA".

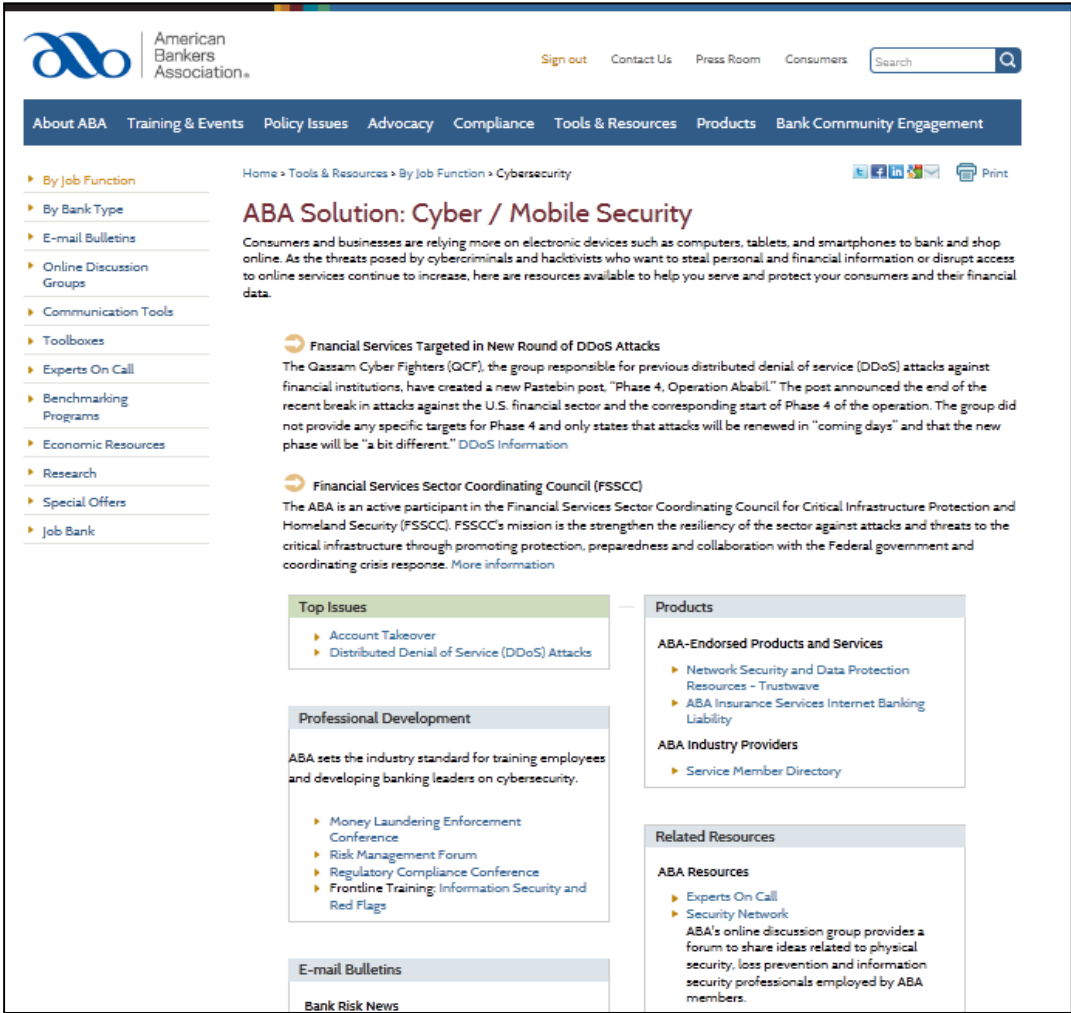
Below the "Get Started" section is a "Get Involved" section with a list of links: "Credit Unions: It's Time to Pay", "Community Bank Reg Relief", "Direct Contact Bankers", and "State Bankers Association Alliance".

The main content area is divided into two columns. The left column is titled "Recent News" and lists three articles: "Trade Deficit Shrinks in June August 6, 2013", "Luetkemeyer Proposes SIFI Designation Changes August 6, 2013", and "ABA Posts Webinar Recording on 'It's Time to Pay' Comms Tools August 6, 2013". Below these is a link for "Survey Finds Some Credit Easing, Stronger Loan Demand August 5, 2013" and a "View All Today's Newsbytes" link.

The right column is titled "Upcoming Events" and lists three events: "Beyond Payroll Cards August 13, 2013 | Briefing", "ABIA Annual Conference September 16-18, 2013 | Ponte Vedra, FL", and "Marketing Conference September 22-24, 2013 | San Antonio". Below these is a link for "Wealth Management & Trust Conference February 26-28, 2014 | San Diego" and a "More Events for Banking Professionals" link.

At the bottom of the page are three promotional boxes. The first is "ABA Experts on Call" with an image of a dart hitting a target and the text "On-target Answers" and "Members-only Access to Banking Experts Search Online Now". The second is "NEW: Cybersecurity Resources" with an image of a padlock and the text "Visit aba.com/Cybersecurity". The third is "Educate. Advocate. CHANGE." with a "Make an Impact: Edit" button and a video player thumbnail.

Cybersecurity Landing Page



The screenshot shows the American Bankers Association's Cybersecurity Landing Page. The page features a navigation menu with categories like 'About ABA', 'Training & Events', 'Policy Issues', 'Advocacy', 'Compliance', 'Tools & Resources', 'Products', and 'Bank Community Engagement'. The main content area is titled 'ABA Solution: Cyber / Mobile Security' and includes a sub-header 'Financial Services Targeted in New Round of DDoS Attacks'. Below this, there are sections for 'Financial Services Sector Coordinating Council (FSSCC)', 'Top Issues', 'Professional Development', 'E-mail Bulletins', 'Products', and 'Related Resources'. The page also includes a search bar and social media links.

American Bankers Association

Sign out | Contact Us | Press Room | Consumers | Search

About ABA | Training & Events | Policy Issues | Advocacy | Compliance | Tools & Resources | Products | Bank Community Engagement

Home > Tools & Resources > By Job Function > Cybersecurity

ABA Solution: Cyber / Mobile Security

Consumers and businesses are relying more on electronic devices such as computers, tablets, and smartphones to bank and shop online. As the threats posed by cybercriminals and hackers who want to steal personal and financial information or disrupt access to online services continue to increase, here are resources available to help you serve and protect your consumers and their financial data.

Financial Services Targeted in New Round of DDoS Attacks

The Qassam Cyber Fighters (QCF), the group responsible for previous distributed denial of service (DDoS) attacks against financial institutions, have created a new Pastebin post, "Phase 4, Operation Ababil." The post announced the end of the recent break in attacks against the U.S. financial sector and the corresponding start of Phase 4 of the operation. The group did not provide any specific targets for Phase 4 and only states that attacks will be renewed in "coming days" and that the new phase will be "a bit different." [DDoS Information](#)

Financial Services Sector Coordinating Council (FSSCC)

The ABA is an active participant in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). FSSCC's mission is to strengthen the resiliency of the sector against attacks and threats to the critical infrastructure through promoting protection, preparedness and collaboration with the Federal government and coordinating crisis response. [More information](#)

Top Issues

- Account Takeover
- Distributed Denial of Service (DDoS) Attacks

Professional Development

ABA sets the industry standard for training employees and developing banking leaders on cybersecurity.

- Money Laundering Enforcement Conference
- Risk Management Forum
- Regulatory Compliance Conference
- Frontline Training: Information Security and Red Flags

E-mail Bulletins

- Bank Risk News

Products

ABA-Endorsed Products and Services

- Network Security and Data Protection Resources - Trustwave
- ABA Insurance Services Internet Banking Liability

ABA Industry Providers

- Service Member Directory

Related Resources

ABA Resources

- Experts On Call
- Security Network

ABA's online discussion group provides a forum to share ideas related to physical security, loss prevention and information security professionals employed by ABA members.

Cybersecurity Issues Pages

The screenshot shows the ABA website's 'Distributed Denial of Service Attacks (DDoS)' page. The page features a navigation menu with categories like 'About ABA', 'Training & Events', 'Policy Issues', 'Advocacy', 'Compliance', 'Tools & Resources', 'Products', and 'Bank Community Engagement'. A sidebar on the left lists various resources such as 'By Job Function', 'By Bank Type', 'E-mail Bulletins', 'Online Discussion Groups', 'Communication Tools', 'Toolboxes', 'Experts On Call', 'Benchmarking Programs', 'Economic Resources', 'Research', 'Special Offers', and 'Job Bank'. The main content area includes a breadcrumb trail: 'Home > Tools & Resources > By Job Function > Fraud / Security > Distributed Denial of Service Attacks (DDoS)'. The page title is 'Distributed Denial of Service Attacks (DDoS) Issue'. The text discusses recent attacks on financial institutions and provides a list of actions: 'Contact the Financial Services (SOC) immediately at iat@fsisa.org', 'Consider tailoring the following', and 'Recommended Consumer Me...'. A section titled 'July 2013' contains an alert: 'Alert: DDoS Attacks May Resume this W... denial of service (DDoS) attacks against fi... post announced the end of the recent bre... operation. The group did not provide any... and that the new phase will be "a bit diffe...'. It also mentions downloading the 'FS-I (DDoS) Attacks' document and provides more information.

The screenshot shows the ABA website's 'Corporate Account Takeover' page. The page features a navigation menu with categories like 'About ABA', 'Training & Events', 'Policy Issues', 'Advocacy', 'Compliance', 'Tools & Resources', 'Products', and 'Bank Community Engagement'. A sidebar on the left lists various resources such as 'By Job Function', 'By Bank Type', 'E-mail Bulletins', 'Online Discussion Groups', 'Communication Tools', 'Toolboxes', 'Experts On Call', 'Benchmarking Programs', 'Economic Resources', 'Research', 'Special Offers', and 'Job Bank'. The main content area includes a breadcrumb trail: 'Home > Tools & Resources > By Job Function > Fraud / Security > Corporate Account Takeover'. The page title is 'Corporate Account Takeover Issue'. The text defines Corporate Account Takeover as a type of corporate identity theft and describes the impact on banks and customers. It provides a list of actions: 'Banks must protect themselves by increasing internal awareness of this fraud, enhancing the ability to monitor for and detect it, and developing a response plan to address it. Most importantly, since banks cannot control the security of their customers' devices, they must work to educate their clients of the risks and how they can protect themselves.' A section titled 'ABA Positions' states that the ABA is committed to addressing this issue through its participation in various collaborative working groups.

New Cybersecurity Category on CAB pages

American Bankers Association logo and navigation menu (Sign out, Contact Us, Press Room, Consumers, Search). Main navigation: About ABA, Training & Events, Policy Issues, Advocacy, Compliance, Tools & Resources, Products, Bank Community Engagement.

Home > CAB

Corporation for American Banking (CAB)

Help banks make money, save money, diversify income and improve efficiency. Backed by thorough due diligence and field-tested and customer-service standards.

ENDORSED PRODUCTS BY CATEGORY

- ▶ Asset Management
- ▶ Compliance/Risk
- ▶ Consulting
- ▶ **Cybersecurity**
- ▶ Credit Risk Management
- ▶ Funding
- ▶ Insurance
- ▶ Marketing/Affinity
- ▶ Technology
- ▶ ABA Member Discounts

View solutions by category ▶
View solutions alphabetically ▶

American Bankers Association logo and navigation menu (Sign out, Contact Us, Press Room, Consumers, Search). Main navigation: About ABA, Training & Events, Policy Issues, Advocacy, Compliance, Tools & Resources, Products, Bank Community Engagement.

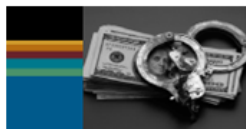
Home > CAB > Solutions

ABA-Endorsed Products and Services

Alphabetical Listing of Products and Services

- ▶ Insurance
 - ▶ ABA Insurance Services- D&O, Bond, P&C Insurance
 - ▶ BOLI Portfolio Solutions
 - ▶ Customer Appreciation Insurance - AD&D
 - ▶ Real Estate and Consumer Loan Insurance
 - ▶ STAMP Surety Bond
- ▶ **Cybersecurity**
 - ▶ Network Security and Data Protection Resources - Trustwave
 - ▶ ABA Insurance Services Internet Banking Liability
- ▶ Technology
 - ▶ ATM and Branch Transformation Solutions
 - ▶ Cash Inventory Software
 - ▶ Check Fraud Reduction Software
 - ▶ Check Imaging Solutions
 - ▶ Core Processing
 - ▶ Deposit Reclassification
 - ▶ EFT/ATM/POS Payments
 - ▶ Employment Screening
 - ▶ FI Performance Management
 - ▶ Network Security and Data Protection Resources
 - ▶ Online Audit Confirmations and Credit Inquiries
 - ▶ Payment Solutions
 - ▶ Technology Solutions by Fiserv

Bank Risk News



Bank Risk News

May 6, 2013

ABA NEWS

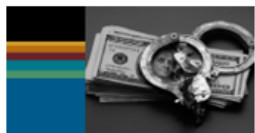
Alert: DDoS Attacks to Target Banks on May 7

The hacker group Anonymous announced that it will launch OperationUSA against banking and government websites. OperationUSA poses a limited threat to the security of Homeland Security, OperationUSA poses a limited threat to the security of Homeland Security.

ABA has revised its Distributed Denial of Service (DDoS) messaging tips and recommended mitigation strategies.

[Read more.](#)

[Read the list of potential targets.](#)



Bank Risk News

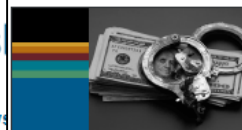
Fraud ... Cybersecurity ... Physical Security ... Emergency Preparedness

May 20, 2103

ABA NEWS

ABA to Testify on Cybersecurity

Charles Blauner, global head of information security at ABA, will testify before a House Energy and Commerce Committee hearing on steps the federal government and industry can take to protect the nation's critical infrastructure and mitigate exposure to cyber threats.



Bank Risk News



Fraud ... Cybersecurity ... Physical Security ... Emergency Preparedness

June 10, 2013

REGULATORY INFORMATION

FFIEC Forms Cybersecurity Working Group

The Federal Financial Institutions Examination Council announced the formation of a working group to better coordinate among banking regulators on cybersecurity and critical infrastructure issues. The group formed in response to the growth in volume and sophistication of cyber attacks and the increasing importance of critical financial infrastructure to financial stability.

Through this group, FFIEC's member agencies will build on existing government and private-sector activities, including FFIEC's Information Technology Subcommittee of the Task Force on Supervision, the Financial and Banking Information Infrastructure Committee, the Financial Services Sector Coordinating Council and the Financial Services Information Sharing and Analysis Center. [Read more.](#)

- Distributed each Monday
- More than 11,000 subscribers
- Archived and monthly compilations posted on ABA.com

ABA Fraud/Scam Report



The following banking-related items were recently reported by the Department of Homeland Security as part of their [Daily Open Source Infrastructure Protection Report](#).

International and National News

8 charged in \$15 million attempted cyber fraud targeting U.S. banking customers
June 12, Dark Reading

A complaint filed by the U.S. Secret Service charged eight individuals in the U.S. and Ukraine with allegedly running a fraud operation that attempted to steal at least \$15 million from U.S. banking customers that included hacking into financial institutions' systems and making fraudulent purchases and ATM withdrawals.

[Read more.](#)

- Distributed each Friday
- Over 5,500 subscribers
- Archived and monthly compilations posted on ABA.com

ABA Security Network

Create a Groupsite | Find a Group

ABA Security Network

American Bankers Association

LOGIN | ABA SECURITY NETWORK | HELP

Login to your Account

About ABA Security Network

We use Groupsite.com for authentication. [What is Groupsite.com?](#)

Email Address

Password

Remember Me [What is this?](#)

[LOG IN](#) [Forgot Password?](#) [Need Login Help?](#)

- An information sharing forum for physical security, loss prevention and information security professionals employed by ABA members
- More than 1,300 subscribers

The Path Forward – 2014/15

1. Evaluate cybersecurity endorsements
2. Grow Cyber and Information Security Working Group
3. Grow electronic bulletins and Security Network
4. Continue to support the FS-ISAC
5. Maintain leadership role in national cyber discussions
6. Build CEO cybersecurity resource
7. Continue customer education/protection efforts
8. Gain ICANN approval to operate .Bank top level domain

Cybersecurity: Awareness, Preparedness and Strategy

Doug Johnson
American Bankers Association